Nejlepší nástroje proti spywaru

Už nikdy spyware

Agresivní špionážní nástroje vyzradí vaše data nejen neseriózním firmám. O své soukromí můžete přijít během pár sekund, aniž byste si toho vůbec povšimli.

Text: Fabian von Keudell, *autor@chip.cz*

Rozblikalo se na vaší ovládací ploše zčistajasna víc reklam než na Nově a Primě dohromady? Pak jste se nejspíš stali obětí „SpyAxe“, nebezpečného špionážního softwaru, který slídí po vašich datech. SpyAxe je v současné době nejagresivnějším zločinným nástrojem svého druhu.

Avšak spyware začaly používat i firmy jinak seriózní. Posledním případem je oblíbený iTunes firmy Apple, který právě přehrávanou skladbu oznámí na web a pak zobrazí cílenou reklamu.

Udělejte tomu konec! Odhalte špiony a staňte se znovu pány svého počítače. Pro boj proti spywaru si vhodné zbraně zvolte sami. Uživatelům, kteří jen tu a tam navštěvují pouze důvěryhodné stránky, postačí kontrola systému jedenkrát týdně. Nejvhodnějším prostředkem je zde SpyBot-Search & Destroy, nekomplikovaný nástroj nenáročný

NAJDETE NA CHIP DVD

- **Spy Sweeper**
  shareware
  www.webroot.com
- **Microsoft AntiSpyware Beta 1**
  freeware
  www.microsoft.com
- **SpyBot Search & Destroy**
  freeware
  www.safer-networking.org
- **CWShredder**
  freeware
  www.spywareinfo.com/~merijn/downloads.html
  www.trendmicro.com/cwshredder/

PĚT ZÁSAD PROTI SPYWARU

Maximální bezpečnost s minimálními náklady. Takto ochráníte svůj počítač před spywarem i v budoucnu.

Nedůvěřujte neznámým programům

Nespouštějte hned každou aplikaci, která se vám dostane do rukou – i kdyby pocházela z důvěryhodného zdroje.

Nainstalujte si antispywarový nástroj

Používejte některý ze zde představených programů a nakonfigurujte jej podle popisu. Jen tak bude skenování spywaru probíhat v reálném čase.

Nahrávejte aktualizace

Vždy nainstalujte nejnovější aktualizace Windows, aby se ve vašem počítači nemohl uhnízdit nový spyware. Totéž platí pro updaty vašeho antivirového programu a nástrojů proti spywaru.

Nainstalujte firewall

Další ochranu proti vetřelcům poskytuje firewall. Ten ukáže, kdy a jak se který program snažil dostat na internet.

Používejte antivirový software

Proti trojským koním, které do systému propašují spyware, pomůže dobrý virový skener.

SpyAxe – nové spywarové nebezpečí

1 SpyAxe svévolně ukládá soubory na váš pevný disk, vytváří tajné položky v systémovém registru a spouští skrytou službu. Nic z toho uživatel nezaznamená.

2 Nyní SpyAxe varuje před údajnou spywarovou infekcí. Kdo na zprávu klikne, nainstaluje tím zpoplatněnou verzi antispywaru – která ovšem proti spywaru nijak nechrání.

na systémové prostředky. Vášniví surfaři by si však měli zajistit hlídání v reálném čase, které po spywaru pátrá neustále. Pro tento účel jsou optimální nástroje Microsoft AntiSpyware a Webroot Spy Sweeper. Výhodou řešení od Microsoftu je, že je lépe začleněno do systému, jeho nevýhodou je však to, že je dosud v beta fázi a v angličtině. Pokud vám tato skutečnost vadí, můžete sáhnout po programu Spy Sweeper, jehož 30ti denní trialverzi najdete na ChipDVD.

SPYBOT-SEARCH & DESTROY

Pro občasnou prověrku systému

Na přítomnost spywaru by měl svůj systém přezkoušet každý uživatel alespoň jednou týdně, neboť dokonce i důvěryhodné stránky nasazují k reklamním účelům tzv. tracking cookies. Tyto drobné datové špiony vyžene z disku SpyBot 1.4. Abyste přitom omylem nezlikvidovali i užitečné cookies, vyplatí se jemné vyladění nástroje.

Nahrání aktualizací

Po instalaci SpyBotu byste nejprve měli uvést jeho databanku do nejnovějšího stavu. V hlavním menu proto klikněte na *Aktualizace* a potom na *Vyhledat aktualizace*. Poté si vyberte, o které aktualizace máte zájem, a klikněte na *Stáhnout aktualizace*. Pokud je spojení s aktualizačním serverem příliš pomalé, můžete pomocí tlačítek vedle tlačítka „Vyhledat aktualizace“ zvolit alternativní spojení.

Nastavení výjimek pro cookies

SpyBot může často vyhlásit falešný poplach, například v případě cookies, které ukládají uživatelská data nějakého „freemaileru“. Aby ty přečkaly systémovou čistku, je třeba založit „White List“ s povolenými cookies. Přejděte do profesionálního režimu tak, že v menu *Režim* kliknete na *Pro pokročilé* a pak aktivujete *Nastavení* | *Ignorovat cookies*. V okně vpravo pak uvidíte všechny cookies usídlené v PC. Zaškrtněte prostě příslušnou položku a cookie bude při příští prohlídce ignorován.

Skenování systému

Nyní už můžete spustit kompletní prověrku systému. Klikněte proto na *Search&Destroy* a stiskněte *Zkontrolovat*. Nalezený spyware bezpečně odstraníte tak, že zvolíte *Opravit vybrané problémy*.

MICROSOFT ANTISPYWARE

Pro chronické surfaře a uvědomělé uživatele

Nástroj od autorů Windows je jedním z nejlepších freewarových řešení na trhu. Vyhledávací stroj a ochranný štít rozpozná téměř každý spyware. Háček je v tom, že program je ještě ve stadiu beta 1 a k dispozici jen v angličtině; finální verze přijde až s Windows Vista. Kdo se tím nenechá odradit, může si program s klidným svědomím nainstalovat.

Aktualizace signatur

Po instalaci je alfou a omegou update spywarových signatur. Bez něj nástroj škodlivé

CWSHREDDER

»COOLWEBSEARCH – POČÍTAČ V OHROŽENÍ

Nestává se často, abychom upozorňovali na nástroj určený jen na odstranění jednoho škůdce. V tomto případě však musíme udělat výjimku. Tato utilita má za sebou slavnou minulost a před sebou (bohužel) i dlouhou budoucnost. Tento malý prográmek (nevyžaduje instalaci) totiž umí ze systému likvidovat velké množství verzí škůdce jménem CoolWebSearch (známého také pod jmény CoolWwwSearch, YouFindAll, WhitePages.ws). Zkušenějším uživatelům, kteří na vlastní kůži zažili invazi tohoto škůdce, se určitě ještě teď třesou kolena – ano, odstranit ho například z Windows XP byl téměř nadlidský úkol. A o tom, že CWShredder dělá svou práci dobře, svědčí i skutečnost, že byl nejprve integrován do programu SpySubstract PRO a v současnosti je součástí **Trend Micro Anti-Spyware 3.0**. „Stand alone" verzi najdete na našem DVD nebo na adrese *www.trendmicro.com/ftp/products/online-tools/cwshredder.exe*.

programy prostě najít nemůže. Aktualizační rutinu spustíte prostřednictvím *File | Check for Updates...*

Kontrola systému

Po aktualizaci signatur můžete přistoupit k prověrce systému. Nevolte k tomu však hned *Run Quick Scan Now*, neboť tento příkaz spouští jen „povrchní skenování". Nejprve upravte skenovací parametry tak, že pod tlačítkem *Scan* kliknete na *Scan options*. V následujícím okně označte *Run a full system scan* a zaškrtněte všechny položky pod volbami *Scan memory locations and running processes* a *Deep scan folders*. To sice prodlouží dobu skenování, kontrola však bude důkladnější. Kompletní skenování pak spustíte přes *Run scan now*.

Náprava škod

Spyware se v systému usazuje na nejrůznějších místech, většinou v systémovém registru. Důsledkem může být například XP vyhledávání, které přestalo fungovat. V takovém případě záškodnický program nejprve odstraňte přezkoušením systému v nástroji Microsoft AntiSpyware. Pokud to problém – v našem případě nefunkční XP vyhledávání – neodstraní, znamená to, že v registru byly zrušeny potřebné položky. Ale žádný strach, s tím si AntiSpyware poradí.

V hlavním okně klikněte na *Advanced Tools* a tam na *Browser Restore*. Zde vidíte přehled všech důležitých položek registru, jak je XP aktuálně používají – a jak by správně měly vypadat. Pokud nějaká položka nesouhlasí s originálem vedle, prostě ji vlevo zaškrtněte a prostřednictvím *Restore* obnovte její původní stav.

Blokování škodlivých procesů

Programátoři spywaru vymýšlejí stále rafinovanější metody, jak své záškodnické produkty co nejlépe ukrýt. A tak ve vašem PC často běží slídičský software, aniž byste o tom měli sebemenší tušení.

Právě proto poskytuje AntiSpyware přehled všech běžících ActiveX a Windows procesů, které můžete deaktivovat kliknutím myší. Prostřednictvím *Advanced Tools* aktivujte *System Explorers*. Pod *Downloaded ActiveX* najdete seznam stažených ActiveX aplikací. Pokud vám některá z nich není povědomá, můžete ji deaktivovat pomocí *Block this ActiveX*. Zde si s klidem můžete i trochu zaexperimentovat.

Zablokované aplikace můžete později snadno zase uvolnit: V menu *Tools* klikněte na *Real-time Protection | View all Blocked Events*, tam označte příslušnou aplikaci a stiskněte tlačítko *Unblock Item*. Platí zde základní pravidlo, že vše, co neznáte, byste měli deaktivovat.

Přesměrování

Spyware má v repertoáru ještě další podlé triky. Po zadání internetové adresy se brow-

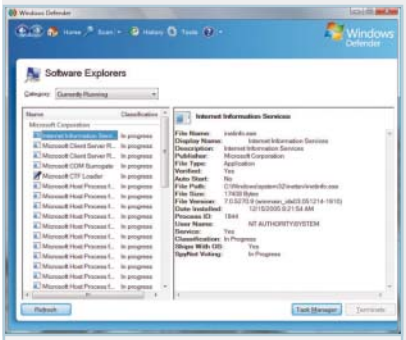
WINDOWS DEFENDER

»OPTIMALIZOVANÁ OCHRANA PROTI SPYWARU VE WINDOWS VISTA

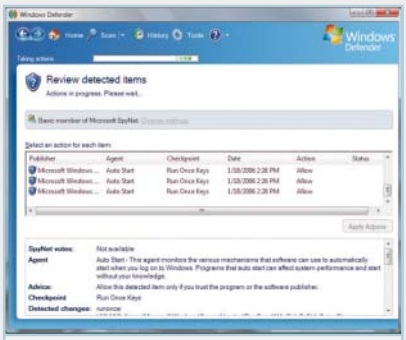
Boj proti spywaru napsal Microsoft na vlajku Windows velkým písmem. Zbraní je Windows Defender, který vznikl konsekventním zdokonalením původního nástroje Microsoft AntiSpyware – jen je ještě elegantněji a hlouběji zakořeněn ve Windows.

Všechna moc patří uživateli: Windows Defender dává uživateli více možností k zásahu. Stěžejní roli přitom hraje Software Explorer. Pomocí něj může uživatel sledovat běžící procesy a získat o nich podrobné informace. Dozví se tak, zda se jedná o službu, nebo o aplikaci, kde je software uložen na disku a která práva procesu přiznává nový systém práv ve Windows Vista. V principu se tedy jedná o rozšířený správce úloh.

Všichni za jednoho, jeden za všechny: Microsoft se chce napříště ještě silněji spoléhat na pomoc uživatelů. Do Windows Defenderu je proto přímo zapojena komunita SpyNet. Tam uživatelé nahlašují nová napadení, Microsoft pak dodá příslušnou signaturu. Praktické je, že aktualizace Defenderu probíhají přes Windows Update, takže nástroj je trvale udržován v nejnovějším stavu. V aktuální beta verzi se Windows Defender váže na bezpečnostní centrum Windows. Díky tomu máte přehled o všech důležitých informacích, od antivirové ochrany přes firewall až po aktuální antispywarový program.



Lepší správce úloh: Nový Software Explorer zobrazuje detailní informace o běžících procesech.



Lepší rozpoznání: Defender odhalí podezřelé programy. V seznamu je můžete deaktivovat.

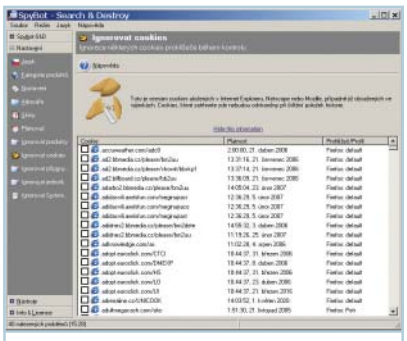
ser nepřipojí k udané URL, ale ukáže úplně jinou stránku. V takovém případě škodlivý program s největší pravděpodobností změnil položky v „hosts“ souboru systému XP. V tomto souboru jsou zaznamenány určité přesměrovací „cesty“. Chcete-li například vybudovat VPN spojení, musí zde být zaznamenána příslušná položka.

Zneužití umožňuje skutečnost, že „okliky“ zaznamenané v Hosts souboru nekontroluje operační systém přes DNS server; zde zaznamenaná spojení mají prioritu. Užitečné opatření, které však v nepovolaných rukou může zcela ochromit síťový provoz.

Chcete-li si záznamy v tomto souboru prohlédnout, v programu AntiSpyware vyvolejte *Advanced Tools* | *System Explorers* | *Windows Hosts File*. Zde můžete kliknutím myší jednotlivé trasy zablokovat nebo úplně zrušit. Také tady platí už zmíněné pravidlo: Neznámé položky zrušit, a až v případě potřeby je znovu zavést.

Problémy

Ani tomuto programu se však nevyhnuly problémy. Už několikrát byl program cílem útoků, které se pokoušely eliminovat jeho činnost. Naposledy se to podařilo trojskému koni jménem BankAsh-A, který potlačoval varovná hlášení a mazal všechny soubory MS Antispywaru v programové složce.



SpyBot umožňuje také vybrané cookies vyřadit z kontroly...

SPY SWEEPER 4.0

Pro profesionální ochranu skenování v reálném čase

Kdo chce svému PC dopřát kompletní ochranu a nedůvěřuje nehotové beta verzi, může se s důvěrou obrátit na Spy Sweeper 4.0. Unikátní devadesátidenní demoverzi tohoto špičkového nástroje také můžete najít na našem DVD.

Aktualizace signatur

Spy Sweeper vyžaduje při updatu zaregistrování u aktualizačního serveru. Po vyřízení této formality spustíte automatickou aktualizaci tak, že v menu *Options* kliknete na *Automatic Check for Updates* a označíte volbu *Automatically download Definition Updates if Available*.

Prověrka systému

Po aktualizaci klikněte v hlavním programu na *Sweep*. Pak zvolte *Start*, čímž spustíte kontrolu systému.

Aktivace automatického skenování

Spy Sweeper umí v určitých časových intervalech provést kompletní prověrku systému samočinně. Nástroj sice nejdůležitější parametry kontroluje v reálném čase, avšak rafinovaný spyware dokáže i přesto najít cestu do systému, například pomocí trojských koní nebo využitím bezpečnostní mezery ve Windows, jako je třeba chyba WMF v XP.

Chcete-li automatickou kompletní prověrku aktivovat, v menu *Options* | *Schedule* klikněte na *Add Scheduled Sweep* a v dalším dialogu pak zadejte, které části pevného disku a s jakou důkladností má Spy Sweeper kontrolovat. Doporučujeme označit všechny skenovací volby – kontrola pak sice trvá déle, ale Spy Sweeper zato najde většinu spywaru. Ještě určete, jak často a kdy má automatické skenování probíhat; zpravidla postačí jednou týdně. Plánovacího asistenta ukončete kliknutím na *Finish*.

Přizpůsobení bezpečnostních voleb

Účinnost Spy Sweeperu lze ještě zvýšit jemnější doladěním. Nejprve aktivujte ochranu proti „tracking cookies“. Nyní přejděte do nabídky *Shields* a tam na kartu *Internet Explorer*. Zde zaškrtněte *IE Tracking Cookies Shield*. Pak si ještě několika kliknutími můžete zajistit ochranu před zrádnými oklikami: v menu *Shields* klikněte na *Hosts File* a aktivujte volbu *Common Ad Sites Shield*.

■ ■ ■

TECHNIKA: SPYWARE POD LUPOU

Kdy vlastně program překročí hranici spywaru? Na to dosud nebyla jednoznačná odpověď. Nyní se ASC (Anti-Spyware Coalition), k jejímž členům patří Microsoft, Symantec, McAfee a HP, konečně dopracovala k odpovědi: Za „pravý“ spyware je považován software, který zaznamenává uživatelská data – bez adekvátního oznámení uživateli, jeho souhlasu nebo kontroly, jak to dělá například iTunes 6.02.
O spyware v širším smyslu se podle definice ASC jedná u technologií, které se svévolně a bez přiměřeného upozornění zapojují do systému, a to tak, že ovlivňují kontrolu uživatele nad následujícími oblastmi: soukromá sféra, bezpečnost systému, využití systémových prostředků, shromažďování, využívání a distribuce soukromých nebo tajných informací. Příkladem tohoto druhu spywaru je rootkit XCP Aurora od Sony.
Zde vám představíme tři nejdůležitější představitele spywaru a ukážeme, jak fungují.

Tracking cookies

Speciální reklamní bannery vysazují do vašeho počítače cookies – agilní obchodníci se tak chtějí dozvědět, v jakých oblastech webu se pohybujete.

Rogue Antispyware

Za domněle prospěšnými protispywarovými nástroji se skrývá sám spyware. Prostřednictvím varování, že v počítači je instalován spyware, na sebe nástroj upozorní a požaduje provedení kontroly systému – přitom však načítá data z počítače.

BHO (Browser Helper Object)

Pod tímto označením je většinou míněna nástrojová lišta pro internetový prohlížeč. Tento jinak užitečný prostředek používají mnohé firmy k tomu, aby získaly informace o vašich surfovacích zájmech. Zpravidla se tento prostředek nainstaluje přes bezpečnostní mezeru typu ActiveX v Internet Exploreru.